Information Security Management System

Internal Audit and Management Review scopes and objectives

Version	Date	Who	What
DRAFT	October 2022	Gary Hinson	Template prepared for SecAware

Summary

ISO/IEC 27001 sections 9.2 and 9.3 specify that **I**nformation **S**ecurity **M**anagement **S**ystems must undergo internal audits and management reviews. This document expands on the scopes and objective of planned ISMS management reviews and audits.

Scopes

Quarter	Management review and internal audit scopes
Q1	**Management review scope:** ISMS information risk assessment activities including their identification and evaluation, excluding the decisions about risk treatment and following activities.
Q2	**Management review scope:** ISMS information risk treatment activities from the point of deciding how best to treat identified-and-evaluated information risks through to their treatment and associated assurance activities (*e.g.* effectiveness monitoring, change management).
Q3	**ISMS internal audit scope:** determine the organisation's readiness for ISO/IEC 27001 certification of the ISMS, identifying any significant areas of concern in sufficient time and detail for them to be resolved *prior* to the certification audit.
Q4	**Management review scope:** information risk and security strategy, ISMS plans and resources for the following year *e.g.* proposals and budgets, priorities.
Q5	**Management review scope:** effectiveness, efficiency and conformity with the ISMS **C**orrective **A**nd **P**reventive **A**ctions process. Is CAPA driving improvements to the organisation's management of information risks, maturing the ISMS at a sensible rate?
Q6	**Management review scope:** value of the ISMS information risk and security metrics. Is suitable, sufficient, relevant, reliable information being generated, passed to the relevant people/functions, and is it in fact being used appropriately to manage the organisation's information risks?

Quarter	Management review and internal audit scopes
Q7	**ISMS internal audit scope:** root cause analysis of [a sample of] ISMS information security incidents and near-misses, looking for common factors and longstanding issues or concerns - particularly systematic or process failings - worth bringing to management's attention. Is now an opportunity to fix things that have been broken for a long time?
Q8	**Management review scope:** information risk and security strategy, ISMS plans and resources for the following year *e.g.* proposals and budgets, priorities.

Objectives

The ISMS reviews and audits share these primary objectives:

- Gain **assurance** that the organisation's information risk and security management arrangements – principally the ISMS – fulfil the requirements of both ISO/IEC 27001 *and* the business (*e.g.* supporting the achievement of business strategies and objectives).
- Identify any issues and concerns requiring management's attention, gathering appropriate evidence and information about probable causes and, if appropriate, recommending changes to improve things.

Supplementary objectives include:

- Ready access to all necessary information;[1]
- Reasonably competent, thorough, professional and objective assessments;[2]
- Collection of sufficient, reliable, factual, credible evidence to substantiate findings, particularly anything significant, contentious, unexpected or persistent;[3]
- Thoughtful, objective, factual analysis and formal reporting, ideally leading to management acceptance and decisions to proceed with changes that improve the business.

Further objectives may be defined as part of the initiation of each assignment, for example:

- Particular issues, concerns or trouble-spots requiring investigation and review;
- Areas to be excluded/ignored for legitimate business reasons;[4]
- Follow-ups on previous audit and review findings, agreed recommendations, unresolved queries, concerns raised by recent incidents *etc*.

[1] This implies substantial trust in those performing the work, with appropriate clearance and oversight.

[2] Within the constraints of resourcing, time and competing priorities.

[3] Evidence, analysis and reports are all likely to be confidential, requiring suitable access controls.

[4] If any, these must be formally discussed and authorised in advance by senior management.